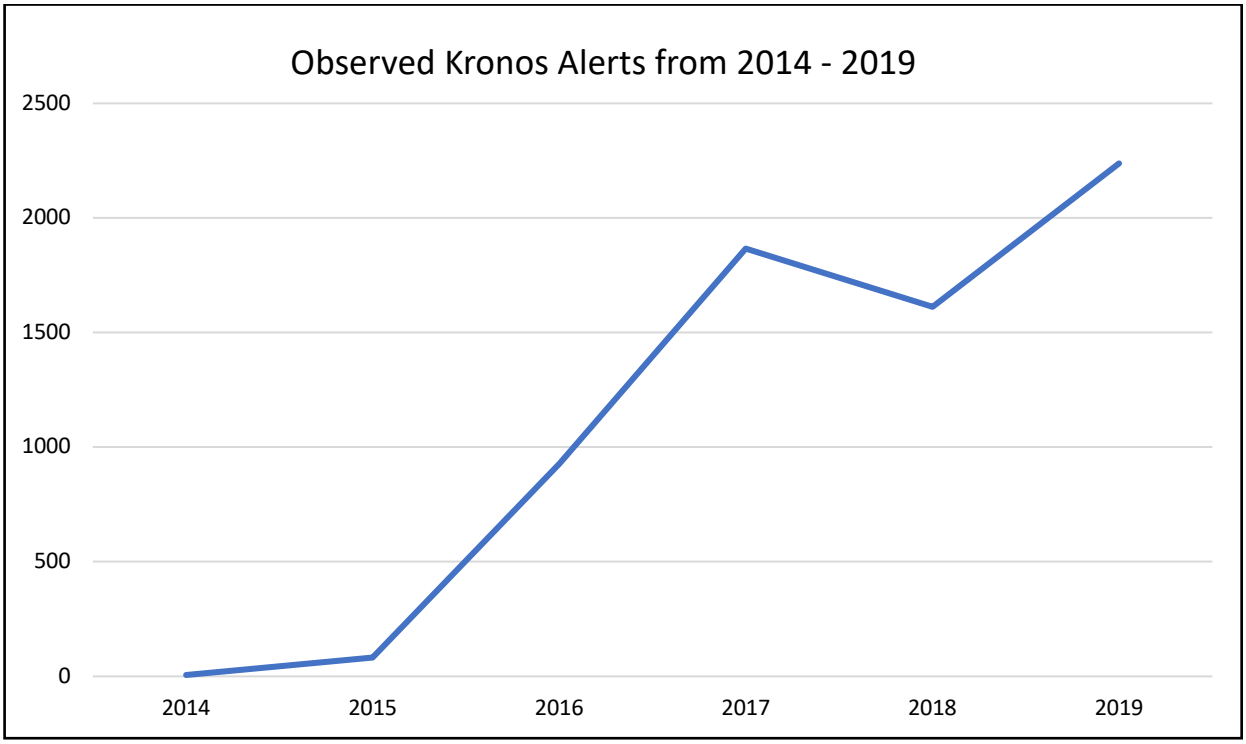
Kronos Trojan Still Active – June 2019

Kronos is a banking malware capable of intercepting web browsing data, injecting its own malicious code into webpages, and downloading additional payloads, while also employing a user-mode rootkit to hide its presence on an infected system.

The Department of Homeland Security and a trusted third party observed Kronos activity in the United States from 2015 – 2019, with increases observed in mid-November 2016 and in quarter two of 2019. Additionally, a spike was observed on federal, state and local networks in quarter four of 2018. It is noted by the trusted third party that it is possible some of the detections are false positives.



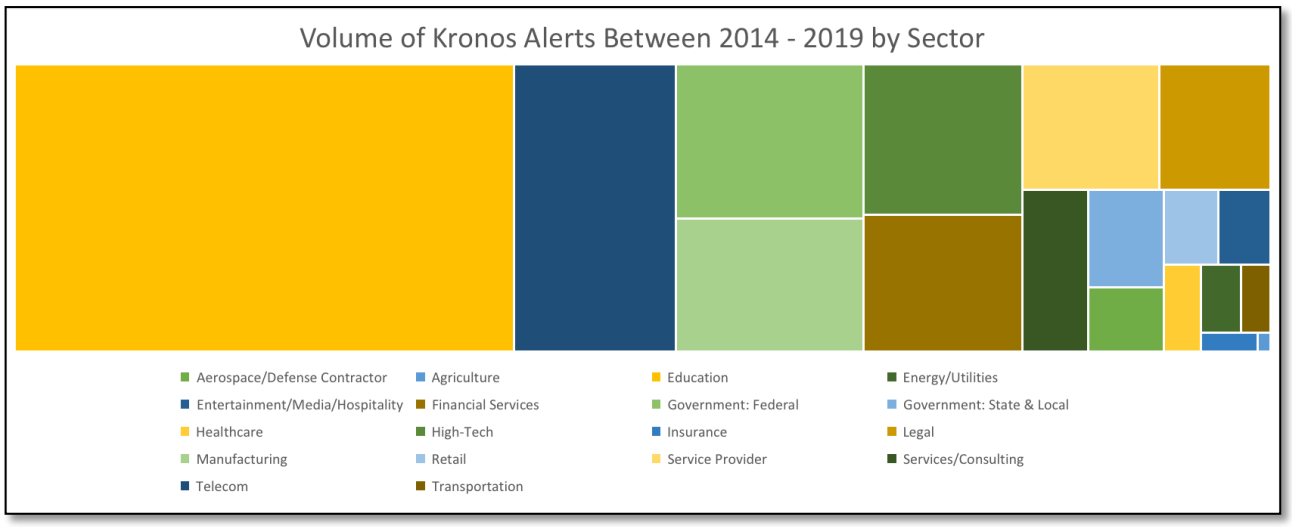
MALWARE HISTORY

The Department of Homeland Security and trusted third parties first observed Kronos advertised on an established Russian cyber-criminal forum by the actor "VinnyK" in June 2014. Like most new banking Trojans to emerge, forum actors were skeptical of its reliability, particularly Russian - speaking actors as VinnyK likely does not speak Russian and was new to the forum. However, it appears that VinnyK commands an adept technical skillset and connections to well-known cyber crime operators.

Kronos botnets have had a modest presence since its initial release in 2014 and are still active today. More recent discussions on underground forums indicate that Kronos licenses cost $3,000 USD, a decrease from its initial price point of $7,000 USD. One Kronos botnet was observed loading a new point-of-sale (POS) malware known as ScanPOS in November 2016. Currently, it appears that several different actors are deploying and maintaining separate Kronos botnets. Several malware customers have been identified hosting C&C on notorious bulletproof hosting infrastructure.

TARGETING

Kronos malware is almost certainly being distributed by multiple customers and, therefore, financial targeting is somewhat geographically distributed. For example, one Kronos botnet hosted on Fluxxy revealed malware infecting hosts in Spain, Romania, Germany, Greece, and the U.S., though overall geographical targeting is more widespread than this. Campaigns have also been observed targeting Canadian and Australian financial institutions. As seen in the below chart, between 2014 – 2019 industries ranging from education, telcom, energy, healthcare and others have been impacted the Kronos Trojan.



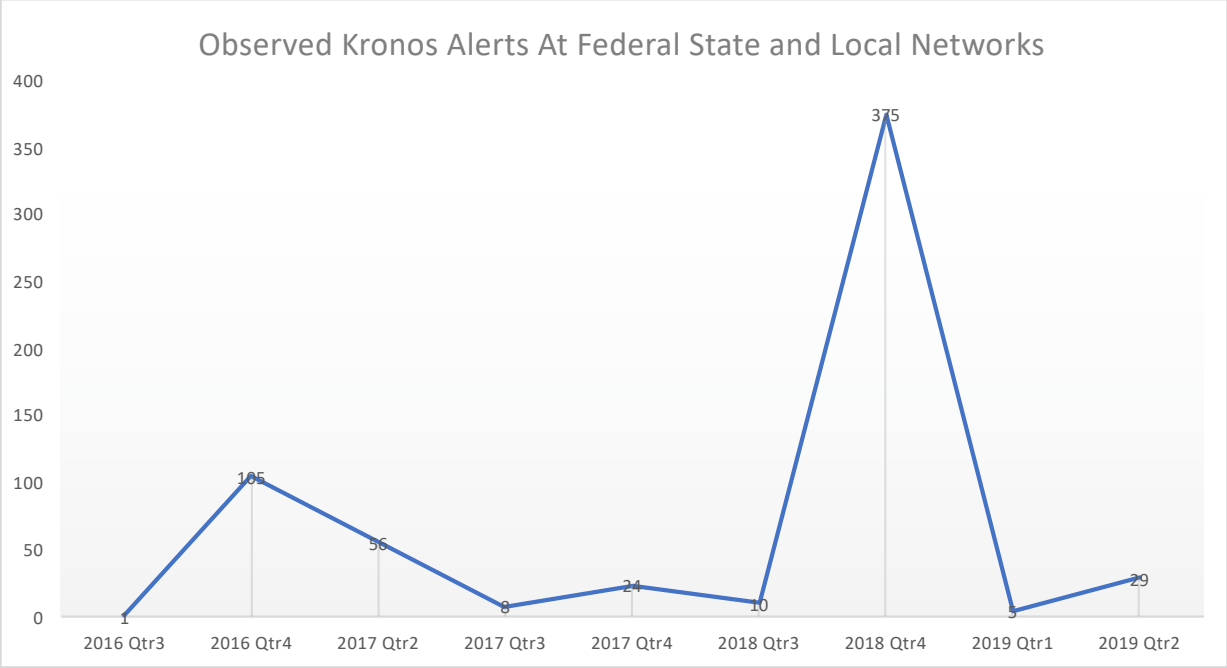
Currently, most Kronos campaign targeting appears to be opportunistic. However, it is noteworthy that a Kronos campaign in 2016 – 2017 delivering ScanPOS appeared to specifically target retail and hospitality sectors in the U.S.

Federal, State and Local Networks

According to a source with first hand access to the information, between the August of 2016 and December of 2017, officials identified Kronos malware activity on U.S. State and local government information systems.

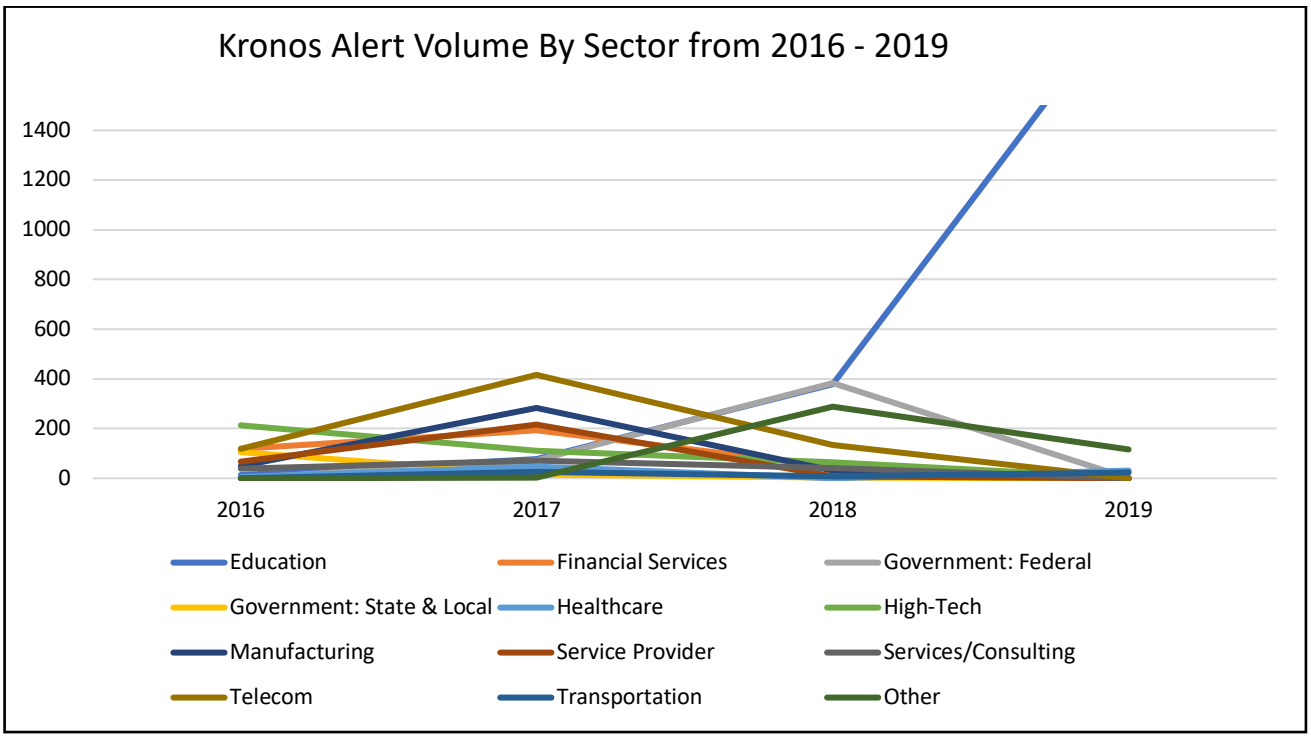
Additionally, multiple states detected and reported cyber reconnaissance and intrusion activity targeting their network that resolved to domains hosting a Kronos C2.

According to a trusted third party, an increase in Kronos alerts on Federal, State and Local networks occurred in quarter 4 of 2018. (Figure 2)



2019 Increase at Education

According to a trusted third party, a large spike in Kronos traffic was observed within the education sector, as noted by figure 4.



MALWARE TECHNICAL OVERVIEW

Kronos is a banking malware capable of intercepting web browsing data, injecting its own malicious code into webpages, and downloading additional payloads. The malware also employs user-mode rootkit code to hide its presence on infected systems.

Upon initial execution, the malware injects its malicious content into a new svchost.exe process and performs several anti-analysis checks. It collects a variety of system information to report back to the C&C server. The original executable is copied into the %APPDATA%\Microsoft\<GUID>\ directory as a hidden file and an associated AutoRun key is generated for persistence.

A new thread is created for opening two sockets: one listening on localhost (127.0.0.1) port 32767 to receive the malware's webinject configuration and intercepted browsing traffic, while the other listens on localhost port 32768 to forward intercepted data to a C&C server or its intended destination after being injected. The local listeners create a proxy that allows the malware to evaluate captured browser traffic, inject its own code into browser webpages, and forward stolen browser data to a C&C server. While these port numbers are hardcoded in the malware, they are incremented during execution as new connections from infected processes are created.

Next, an embedded DLL capable of stealing browsing data from popular browsers is loaded into memory. The malware creates a new thread that injects the DLL into any instance of iexplore.exe, chrome.exe, firefox.exe, or opera.exe. It hooks numerous specified functions, which allows the malware to hijack browser socket connections and redirect their data to a local listener on a specified port. Next, the malware begins hooking functions within browser and system DLLs based on the process into which it was injected. Intercepted network traffic is directed to the local listening port written to the DLL prior to its injection.

The injected svchost.exe process attempts to hide the existence of the malware on the system by injecting user-mode rootkit shellcode into all running processes. The shellcode accomplishes this by hooking several ntdll.dll functions. The hooking code hides the currently running malware process, based on process ID, and other malware artifacts, such as registry keys used and the location of the malware binary on disk.

The malware attempts to communicate with a C&C server every 10 seconds. Each C&C URL is contacted up to three times. If a valid response is not received in three attempts, the next C&C URL is contacted. This continues until the C&C list is exhausted or a valid C&C response is received, at which point the malware sleeps for 15 minutes and begins this process again.

The malware decodes a C&C server's response using a single-byte XOR key found at offset 0x01 within the response.

Once the configuration is successfully downloaded from the C&C and written to disk, the malware sends the plaintext configuration to its own socket listening on a localhost port. The decrypted configuration likely contains webinject HTML code used to perform man-in-the-browser (MiTB) attacks, which allow the malware to alter communications to webpages and steal browsing-related information.

CONCLUSION

The Kronos Trojan has persisted globally from 2014 to 2019.